Remarks

This response is being filed in conjunction with a Request for Continued Examination.

Claims 1-13, 15-27, and 29-41 are pending, with claims 1, 15, and 29 being independent. Claims 14, 28, and 42 are cancelled by this amendment without any waiver or prejudice.

Claims 1-6, 9-13, 15-20, 23-27, 29-34 and 37-41 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bhandal et al. (U.S. Patent No. 6,711,602). Applicants have amended independent claims 1, 15, and 29 to obviate this rejection.

As amended, independent claim 1 recites a multiply unit that includes, among other features, an arithmetic multiplier, a binary polynomial multiplier, permutation logic connected to receive one or more input operands and operable to produce an output that includes a permutation of the one or more input operands, and a multiply unit output data path that is connected to receive an output of the arithmetic multiplier, connected to receive an output of the binary polynomial multiplier, and connected to receive the output of the permutation logic.

Applicants requests reconsideration and withdrawal of this rejection because Bhandal does not describe or suggest permutation logic that is connected to receive one or more input operands and is operable to produce an output that includes a permutation of the one or more input operands. Also, Bhandal does not describe or suggest a multiply unit output data path that is connected to receive an output of the arithmetic multiplier, connected to receive an output of the binary polynomial multiplier, and connected to receive the output of the permutation logic. Instead, Bhandal describes permutation logic, where the output of the permutation logic is used to provide inputs to the Galois multiply unit 164 and the M multiply unit 171. See Bhandal, Fig. 5. Thus, in Bhandal, the permutation logic operation is not performed in parallel along with the operations performed by the Galois multiply unit and the M multiply unit. Rather, the permutation logic is performed and the output is then used as input for the other operations.

Moreover, the Office Action acknowledges that Bhandal "do[es] not disclose a permutation logic connected to receive the one or more input operands and operable to produce an output comprising a permutation of the one or more input operands." See Office Action mailed April 22, 2004 at p. 9, para. 7.

Furthermore, it would not have been obvious to modify Bhandal in view of any other reference to reject amended independent claim 1. Although the Office Action relies upon the Zhijie reference to describe permutation logic, Zhijie would not have led one to modify Bhandal to produce the claimed subject matter because at least one feature of amended independent claim 1 is not described by the combination of Bhandal and Zhijie. In particular, Bhandal and Zhijie, either alone or in combination, fail to describe or suggest a multiply unit output data path that is connected to receive an output of the arithmetic multiplier, connected to receive an output of the binary polynomial multiplier, and connected to receive the output of the permutation logic. Furthermore, a person skilled in the art would not be motivated to modify Bhandal using the teachings of Zhijie, because Bhandal already describes a permutation logic, where the output of the permutation logic is used as input for the M multiply unit and the Galois multiply unit. There is no description or suggestion in either reference to include the permutation logic as a separate operation that is parallel to the operations of the M multiply unit and the Galois multiply unit, especially in light of Bhandal already describing a permutation logic operation that is not in parallel with these other operations.

Like amended independent claim 1, each of amended independent claims 15 and 29 recites an arrangement that includes permutation logic connected to receive one or more input operands and operable to produce an output that includes a permutation of the one or more input operands, and a multiply unit output data path that is connected to receive an output of an arithmetic multiplier, connected to receive an output of a binary polynomial multiplier, and connected to receive the output of the permutation logic.

For at least these reasons, applicants respectfully request withdrawal of the § 102(e) rejections of amended independent claims 1, 15, and 29, and their respective dependent claims.

Claims 7, 8, 21, 22, 35, and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bhandal in view of Magar (U.S. Patent No. 4,538,239). Applicants respectfully request reconsideration and withdrawal of this rejection because Magar does not remedy the failure of Bhandal to describe or suggest the subject matter of the amended independent claims.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 11/24/2004

Joseph P. Key
Reg. No. 44,827

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

40242206.doc